IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) An intrusion detection and analysis system comprising:

a data monitoring device comprising a capture engine operable to capture data passing through the network in response to a trigger and configured to monitor network traffic, decode protocols for grouping packets into different protocol presentations and assembling the packets into high level protocol groups, and analyze received data for managing the network by collecting statistics, and detecting broken lines, traffic loads, and network errors;

an intrusion detection device separate from the data monitoring device, the intrusion detection device comprising a detection engine operable to perform intrusion detection on data provided by the data monitoring device;

application program interfaces configured to allow the intrusion detection device access to applications of the data monitoring device to perform intrusion detection; and

memory for storing reference network information used by the intrusion detection device to determine if an intrusion has occurred;

wherein the application program interfaces allow the intrusion detection device to leverage the separate data monitoring device, by allowing the intrusion detection device to call an application program interface configured to open a protocol decoding application associated with the separate data monitoring device, and by allowing the intrusion detection device to call an application program interface configured to open an alarm generation application associated with the separate data monitoring device.

2. (Original) The system of claim 1 wherein the reference network information comprises a signature database including signature profiles associated with a known network security violation and wherein the detection engine is operable to compare the

data provided by the data monitoring device with the signature profiles to detect network intrusions.

3. (Original) The system of claim 2 further comprising a parser operable to parse, generate, and load signatures at the detection engine.

4. (Original) The system of claim 1 wherein the reference network information comprises a baseline state of network traffic and wherein the detect engine is operable to compare the data received by the capture engine to the baseline network state and look for anomalies.

5. (Original) The system of claim 4 wherein the data monitoring device provides the baseline state of network traffic.

6. (Original) The system of claim 1 further comprising a log file configured to at least temporarily store reports generated by the detect engine.

7. (Original) The system of claim 6 further comprising an alarm manager operable to generate alarms based on information generated by the log file.

8. (Original) The system of claim 1 further comprising a filter configured to filter out packets received at the data monitoring device.

9. (Cancelled)

10. (Original) The system of claim 1 wherein the capture engine is configured to forward packets and temporarily store packets for later analysis by the data monitoring device.

11. (Currently Amended) A method for performing intrusion detection with an intrusion detection and analysis system comprising a data monitoring device including a capture engine operable to capture data passing through the network in response to a trigger and configured to monitor network traffic, decode protocols for grouping packets into different protocol presentations and assembling the packets into high level protocol groups, and analyze received data for managing the network by collecting statistics, and detecting broken lines, traffic loads, and network errors, and an intrusion detection device separate from the data monitoring device, the intrusion detection device coupled to the data monitoring device and configured to perform intrusion detection on data provided by the data monitoring device; the method comprising:

receiving data at the data monitoring device;

capturing at least a portion of the packets contained within the data;

by allowing the intrusion detection device to call [an]at least one application program interface configured to open applications of the data monitoring device; and

performing intrusion detection at the intrusion detection device utilizing at least one of the applications of the data monitoring device;

wherein the at least one application program interface allows the intrusion detection device to leverage the separate data monitoring device, by allowing the intrusion detection device to call an application program interface configured to open a protocol decoding application associated with the separate data monitoring device, and by allowing the intrusion detection device to call an application program interface configured to open an alarm generation application associated with the separate data monitoring device.

12. (Cancelled)

13. (Cancelled)

14. (Original) The method of claim 11 further comprising filtering the data prior to capturing packets.

15. (Original) The method of claim 11 wherein performing intrusion detection comprises performing signature matching.

16. (Original) The method of claim 15 wherein the application program interfaces provide parsing of signatures used in signature matching.

17. (Cancelled)

18. (Original) The method of claim 11 wherein performing intrusion detection comprises detecting anomalies in the received data.

19. (Currently Amended) A computer program product for performing intrusion detection with an intrusion detection and analysis system comprising a data monitoring device including a capture engine operable to capture data passing through the network in response to a trigger and configured to monitor network traffic, decode protocols for grouping packets into different protocol presentations and assembling the packets into high level protocol groups, and analyze received data for managing the network by collecting statistics, and detecting broken lines, traffic loads, and network errors, and an intrusion detection device separate from the data monitoring device, the intrusion detection device coupled to the data monitoring device and configured to perform intrusion detection on data provided by the data monitoring device; the product comprising:

code that receives data at the data monitoring device;

code that captures at least a portion of the packets contained within the data;

code that calls [an]at least one application program interface configured to open applications of the data monitoring device;

code that performs intrusion detection at the intrusion detection device utilizing at least one of the applications of the data monitoring device; and

a computer-readable storage medium for storing the codes;

wherein the at least one application program interface allows the intrusion detection device to leverage the separate data monitoring device, by allowing the intrusion detection device to call an application program interface configured to open a protocol decoding application associated with the separate data monitoring device, and by allowing the intrusion detection device to call an application program interface configured to open an alarm generation application associated with the separate data monitoring device.

20. (Currently Amended) The computer program product of claim 19 wherein the computer readable storage medium is selected from the group consisting of CD-ROM, floppy disk, tape, flash memory, system memory, and hard drive~~, and data signal embodied in a carrier wave~~.

21. (New) The system of claim 1 wherein at least one of the application program interfaces take the form of frame_context_pointer_position.

22. (New) The system of claim 1 wherein at least one of the application program interfaces include:
frame_tcp_bridge,
frame_udp_bridge,
frame_ip_bridge, and
frame_http_bridge.